REMARKS

Claims 1-30 are pending and are unamended.

Request for Interview Prior to Formal Action on Response

Applicants request an interview prior to formal action on this response. An "Applicant Initiated Interview Request Form" accompanies this response. Please contact Applicants' undersigned representative to schedule the interview.

Although Applicants have conducted previous interviews with the Examiner, the present grounds of rejection are entirely new.

Rejections under 35 U.S.C. § 102

1. Patentability of claims 1-30 over Buck

All pending claims were rejected under 35 U.S.C. § 102(e) as allegedly being anticipated by U.S. Patent Application Publication No. 2002/0055912 (Buck). Applicants respectfully traverse this rejection.

Applicants present a "Declaration of Prior Invention to Overcome Cited Patent" under 37 CFR § 1.131 to swear behind the earliest potential effective date of Buck, which is October 20, 2000, the date of Buck's provisional application.

The Declaration paperwork is self-explanatory. However, to briefly summarize the paperwork, it establishes that the claimed invention was reduced to practice prior to the earliest possible effective date of Buck, namely, October 20, 2002. Prior to October 20, 2002, and as evidenced by the Declaration exhibits, the software code for Applicants' invention was completed and beta tested, and a commercial product based on the software code was commercially released. In view of the Declaration, withdrawal of the rejection over Buck is respectfully requested.

2. Patentability of claims 1 and 16 over Norton Internet Security 2000, hereafter, "NIS 2000"

Claims 1 and 16 were rejected as allegedly being anticipated by NIS 2000. Applicants respectfully traverse this rejection.

The Examiner asserts that the "Black web site list" in NIS 2000 is equivalent to the claimed "list of cookie file sources." Applicants respectfully disagree. The Black web site list in NIS 2000 is merely a list of web sites that NIS has designated as web sites that a user should not be permitted to navigate to. The web sites may or may not have cookies. Thus, any particular download of the latest Black web site list may include no web sites that are cookie file sources. If any of the web sites on the Black web site list is a cookie file source, then it is just coincidental, since NIS 2000 makes no effort to specifically identify cookie file sources. In fact, cookie control is a completely different feature in NIS 2000, which is independent of the Black web site list. See, paragraph 1 on page 3 of 5 of Jay which reads as follows (underlining added for emphasis):

> It'll also prevent children to access potential harmful risk websites or even chat software (or even email software; you can tweak easily this setting). NIS comes with a one year of free updates to ensure that you've always got the latest 'Black web site list' thanks to its LiveUpdate technology....NIS can even block Cookies, but with this feature enabled a lot of websites will refuse to work, as they required a cookie to save users preferences...

Claims 1 and 16 explicitly recite a step of a subscriber requesting from a server a "list of cookie file sources," not a list of potentially bad web sites that may or may not be cookie file sources. Step (a) of claims 1 and 16 are thus directed to a completely different invention than the Black web site list of NIS 2000.

Since NIS 2000 does not disclose or suggest step (a) of claims 1 and 16, NIS 2000 inherently cannot disclose or suggest step (b) of claims 1 and 16.

The Examiner further asserts that the cookie blocking function in NIS 2000 is equivalent to the claimed step (c) of using the downloaded list of cookie file sources to detect cookie files received at a client machine from sources on the downloaded list. Applicants respectfully disagree.

Referring to excerpt from Jay above, NIS 2000 does not block cookies by comparing the source of the cookies with the Black web site list, or with any list at all. That is, there is no relationship between the Black web site list and which cookies get blocked since these features are unrelated to each other. (Of course, if a web site is on the Black list and contains a cookie, then that cookie will be blocked, but only as a coincidence of being on the Black list, and not because it was on a list of cookie file sources.) Instead, Jay merely states that NIS 2000 can be set to block cookies (presumably, all cookies) or not to block any cookies. Jay even points out that blocking cookies can prevent a lot of websites from working with the user. Stated simply, merely blocking cookies is not equivalent to the functionality recited in step (c).

In sum, NIS 2000 does not disclose or suggest any of the three steps in claims 1 and 16, and thus these claims are believed to be patentable over NIS 2000.

3. Patentability of claims 1 and 16 over Howard et al., hereafter, "Howard"

Claims 1 and 16 were rejected as allegedly being anticipated by Howard. Applicants respectfully traverse this rejection.

The Examiner highlights column 7, lines 25-40 of Howard as allegedly disclosing all three of the claimed steps. Column 7, lines 16-40 of Howard reads as follows (underlining added for emphasis):

> If the user-entered information is correct (i.e., matches the information stored in the authentication database) then the authentication server copies the appropriate cookies to the client computer system and redirects the user's browser to the affiliate server (step 212). A "cookie" is a piece of data provided to a web browser by a web server. The data (i.e., cookie) is sent back to the web server by the web browser during subsequent accesses to the web server. With respect to step 212, one cookie contains information regarding the date and time that the user was authenticated by the authentication server. Another cookie contains information regarding the user profile. The authentication server also updates (or creates) a cookie that contains a list of all sites (or web servers) visited by the user since the last logout from the authentication server. The cookie is updated by adding the current affiliate server to the list of sites visited. This list of sites visited is used to remove cookies from the client computer system when the user logs out of the authentication server. For example, when the user logs out, the authentication server

> sends a message to each web server on the list of sites visited. Each message is a request for the web server to delete any cookies it placed on the client computer system (e.g., through a browser running on the client computer system).

The "list" referred to in Howard is merely a list of all web sites visited by the user since the last logout from the authentication server. (The list is contained within a cookie.) The web sites on the list may or may not have cookies. Thus, any particular list may include no web sites that are cookie file sources. The "list" in Howard thus suffers from the same deficiency highlighted above regarding the Black web site list in NIS 2000.

Claims 1 and 16 explicitly recite a step of a subscriber requesting from a server a "list of cookie file sources," not a list of web sites visited by the user that may or may not be cookie file sources.

Furthermore, Howard does not even disclose that a subscriber (user) requests to send the list to the client machine (client computer system). Column 7, lines 16-40 and the corresponding figures merely describe and show that an authentication server updates/creates the list of visited sites and uses the list to direct the visited sites to delete any cookies that they placed on the client computer system. However, even if it assumed that the list is somehow propagated to the client computer system, at best, Howard would then merely disclose a step of "receiving, at a server, a request from a subscriber to send a list of web sites visited by the user to a client machine," not a list of cookie file sources as claimed. Stated simply, the claimed request for a list of cookie file sources is not a request for a list of visited web sites that may or may not have sent a cookie as part of the visit. Step (a) of claims 1 and 16 are thus directed to a completely different invention than the list in Howard.

Since Howard does not disclose or suggest step (a) of claims 1 and 16, Howard inherently cannot disclose or suggest steps (b) or (c) of claims 1 and 16.

Nonetheless, the Examiner further asserts that column 7, lines 25-40 of Howard discloses the claimed step (c) of using a downloaded list of cookie file sources to detect cookie files received at a client machine from sources on a downloaded list. Applicants respectfully disagree.

Howard states that the "list of sites visited is used to remove cookies from the client computer system when the user logs out of the authentication server." Howard further describes

an exemplary removal process wherein when the user logs out, the authentication server sends a message to each web server on the list of sites visited, each message being a request for the web server to delete any cookies it placed on the client computer system. This process does not involve using a downloaded list of cookie files sources to detect cookie files received at the client computer system from sources on the downloaded list (i.e., a downloaded list of cookie file sources). In fact, no detection of cookie files is even described in Howard. Howard merely instructs the visited web sites to remove any cookies that they placed on the client computer system.

In sum, Howard does not disclose or suggest any of the three steps in claims 1 and 16, and thus these claims are believed to be patentable over Howard.

Conclusion

Insofar as the Examiner's rejections were fully addressed, the instant application is in condition for allowance. Issuance of a Notice of Allowability of all pending claims is therefore earnestly solicited.

Respectively submitted,

Adam R. Schran *et al.*

April 6, 2006 By: Clark Jablon
(Date)

CLARK A. JABLON
Registration No. 35,039
AKIN GUMP STRAUSS HAUER & FELD LLP
One Commerce Square
2005 Market Street, Suite 2200
Philadelphia, PA 19103-7013
Telephone: 215-965-1200
Direct Dial: 215-965-1293